LAM VINSON & COMPANY, LLP
CERTIFIED PUBLIC ACCOUNTANTS
& BUSINESS ADVISORS

May 12, 2005

FFIEC, Program Coordinator
3501 Fairfax Drive, Room 3086
Arlington, VA 22226

Via E-Mail to: FFIEC-Comments@fdic.gov

re: **FIL-41-2005: External Audit Engagement Letters**

Ladies and Gentlemen:

I have received and reviewed the referenced Financial Institution Letter and would like to offer comments thereon for your consideration.

In general, I wholeheartedly support accountability for professional performance. I believe that the accounting profession's attest function has fallen victim to a host of problems, many of which have been highly publicized and only partially addressed. However, one of the most detrimental influences has also had the same impact on regulatory responsibility. A clear lack of consistent enforcement of rules and regulations has made chumps out of those that strive to act professionally and/or comply – that includes auditors and bankers. "Natural adverse selection" of unprofessional auditors subordinate to management desires is the root cause of virtually all auditor independence issues. Straining gnats such as the limited liability provisions that are the subject of this FIL are further contributory because they distract attention from the real issue.

Professional performance and compliance require experience and expertise, neither of which are cheap. Therefore, when individuals and/or entities that fail to comply are given a pass, a slap on the wrist or a warning not to do it again, they have won and those that strove to comply have lost. The offenders have saved substantial costs (even if they then begin to comply) while the true professionals and compliant institutions have, from a "business" perspective, incurred unnecessary costs with little or no reward. In fact, in the case of an auditor that strives to act professionally and fulfill his or her responsibility to the Board, audit committee ("**AC**"), investors, depositors, regulators and the public as taxpayers, he or she actually finds professionalism to be a detriment to his/her business.

This is the most important and pervasive cause of what FIL-41-2005 cites as weakened external auditor objectivity, impartiality and performance that results in unsafe and unsound practice. This is more pervasive in smaller institutions (i.e., under $500 Million) due to the enforcement resources directed at these institutions, but remains a significant problem with many larger institutions. Practically speaking, the external auditors are hired, evaluated and fired by the people they are supposed to be auditing – which is absurd on its face.

The end result of this approach is predictable and manifest as the source of the many highly publicized problems plaguing our financial markets. If an auditor comes in and criticizes management, he/she is terminated and replaced with another, less diligent auditor; i.e., an auditor that realizes who pays them. The reputation of the auditor that was terminated is then tarnished and it becomes even harder to get engaged. The auditor that complies with management's every whim is praised in the banking community and his/her practice flourishes. There are a few exceptional organizations that do not operate this way, but they truly are exceptional and rare.

Practically, AC's have little or no impact on this problem because of lack of competence, independence and involvement. Even when financial institutions have an AC, the AC subordinates judgment to management because (i) they often have no understanding of bank accounting or financial reporting, (ii) even more often they have no understanding of the purpose or scope of a financial statement audit and (iii) the rule of reality continues to be that management determines who is on the AC and who stays on the AC (regardless of what the policy and organization chart say).

The new PCAOB requirements for ACs to have "at least one" financial expert is very revealing. The definition of financial expert actually only identifies a competent AC member, not a "SuperMember." Therefore, the new rules are basically admitting that, even upon compliance, ACs are likely to include only one competent person (competence here is in reference to their duties as an AC member).

If you are going to rely on ACs to ensure auditor independence and competence, then the AC members must be competent and independent themselves and they must put in enough time to fulfill their responsibilities. Therefore, I believe you should require ACs for all institutions and that they be comprised entirely of independent and competent members.

This situation is then compounded by regulatory endorsement or, at least, acceptance by inaction. Board and AC incompetence is so obvious it is ridiculous, yet there is no regulatory action. Further, most bank regulators have no idea what a GAAS audit is, what an auditor's responsibilities are or the limitations of the scope of their work and, therefore, have no basis on which to evaluate their performance. I have seen it over and over throughout the years and had personal experience with this during the past year. My firm followed another firm on an audit of a financial institution that had been under a C&D and then MOU. This financial institution had hired their external audit firm partner (as CFO), manager (head of the new Internal Audit Department) and one of the staff. The board minutes clearly documented that the previous external audit firm's engagement manager had been hired as the head of the institution's internal audit before that firm's audit report was issued for the prior year. This is a clear and documented violation of professional independence standards (and common sense). The regulatory team was well aware of this because they were sitting in the board meeting when I discussed this matter with the board.

In the course of our audit, we identified almost 40 audit adjustments (totaling millions of dollars) and uncovered a fraud that management concealed from us and the regulatory review team onsite at the same time we were performing our audit. We were terminated prior to issuing our report. The previous audit firm, who still owed the prior audit partner (now the CFO of the institution) for purchasing his practice, was rehired as the auditor. They basically reviewed our workpapers, passed on the millions of dollars in adjustments we had identified and issued a clean opinion (it is important to note that many of the adjustments we identified had been identified and waived in the prior year by that same prior audit firm and even though the current CFO of the institution was the audit partner on that previous audit and had identified many of these adjustments, they remained uncorrected). Even in those obviously extreme circumstances, no regulator ever came to review our workpapers or the other audit firm's workpapers. There was no regulatory objection to the return to an audit firm that issued the opinion the institution desired, even though they knew that firm was not independent when they issued the prior audit report. You don't need new independence rules, you need to enforce what is already there.

Another example of this same regulatory endorsement has to do with periodicity (and I have several actual examples to support this). If a bank's allowance is materially inadequate at 12-31-X1, the financial statement auditor should require a correction in the X1 financial statements or qualify his/her opinion, otherwise the X1 results of operations (net income) are materially misstated. However, the regulatory team that may be performing an exam as of the same date will be perfectly happy if the correction is recorded in the 3-31-X2 call report. Now the auditor has to go to management to require an adjustment as of 12-31-X1 and management's response is – well the regulators are not making us do that. The

auditor is fired and another one is hired. There is no regulatory reaction. However, if the Bank fails or demonstrates capital problems, then the regulators want to blame the auditor for not doing his job and sue for recovery. This is scape-goat logic with very little preventive value.

Unfortunately, particularly in the smaller institutions, this is par for the course. The lack of enforcement by the profession and regulators has created an environment that not only allows this to occur, but actually encourages it through attrition in the ranks of audit firms that seek to do their job and competitive disadvantages to compliant-minded bankers ("natural adverse selection").

Another example of this problem is the discrepancy that has arisen between the scope and cost differences between a PCAOB internal control audit and a FDIC§363 internal control examination under the AICPA's attestation standards. The responsibilities acknowledged in the written reports generated under the PCAOB and AICPA rules are very similar and the distinctions would be lost on the average reader. However, due to virtually complete lack of enforcement under FDICIA (other than checking to see that a copy of the auditor's internal control examination report was obtained), the amount of work performed to support these reports has deteriorated. This is evidenced by the internal costs and external audit fee differences between PCAOB/Sarbanes-Oxley engagements and FDICIA engagements. There is no comparison between the nature and extent of work that goes into these two variations of an internal control audit. The real reason has little to do with actual differences in the regulations and a lot to do with the relatively unknown risk presented by PCAOB review of the public bank's auditor versus the known lack of risk presented by regulatory review of a FDICIA engagement auditor which has extended to the profession's peer review process because, if the regulators don't care about FIDCIA internal control, why should they?

Another example is the FFIEC Policy on External Audits. In Texas and across the country, "Director's Exam's" are routinely performed and accepted, even though the FFIEC policy does not include them as an acceptable alternative, rather a financial statement audit, balance sheet audit or internal control examination are indicated as acceptable alternatives. Although I'm sure there is no need, I can give you actual examples of banks under $100 million that have a GAAS audit performed annually, while there are banks approaching $500 million that still have a "Director's Exam." Also, in this so-called policy, it is recommended for all banks to have an external audit. Again, compliant-minded banks incur the cost, non-compliant banks do not. "Suggestive regulations" are detrimental because they feed natural adverse selection – greater compliance by banks that are not a problem in the first place and the banks that need it pay no heed.

FIL-41-2005 also suggests some misunderstanding of the scope of a GAAS audit. In part *IV. Proposed Advisory*, the first paragraph under the *Background* subsection, the FIL states "…When planning and performing the audit, the external auditor considers the financial institution's internal control over financial reporting. Generally, the external auditor communicates any identified deficiencies in internal control to management, which enables management to take appropriate corrective action…" This reference in the FIL perpetuates and magnifies a misperception that a GAAS audit includes tests of controls. The statement in the FIL is deceptive. A GAAS financial statement audit generally does not include any tests of controls. In a GAAS audit, the external auditor does "consider the financial institution's internal control" as part of the audit, but only to the extent necessary to "plan" the audit. Since virtually all GAAS audits outside of FDIC§363 do not "rely on the institution's internal control," the external auditor appropriately does very little in regard to internal control. In fact, any recommendations on internal control are highly incidental to the process. Under GAAS, if an auditor does not plan to rely on a bank's internal control, there will be no tests of internal control; therefore, at best the auditor might identify blatant *design* deficiencies, but would have virtually no likelihood of identifying *operating* deficiencies.

This alludes to a pervasive problem with regulatory monitoring approaches. Written policies and procedures are required by regulators, which on the surface would appear to be a good thing. However, actual compliance with those policies and procedures is rarely tested, and if it is, it is by inquiry only (i.e., no detail tests of controls). Any banker that's been around the block once knows you just go buy "canned" policies and procedures and the regulators are happy. If you have a piece of paper to hand them when asked, they can check that item off the list and move on.

While I wholeheartedly agree that professionals (including external auditors) should be accountable for professional performance, I think the effect of this FIL will be merely to extrapolate the misunderstandings surrounding external auditor responsibility and expose auditor's to liability for matters that are not their responsibility. One has to wonder if the latter is not the intent?

Auditors that competently and diligently perform their duties cost more than those that do not – another competitive disadvantage (guess what the primary criterion the non-compliant-minded organization is going to apply when they hire an auditor – cost, not competence, ability and performance – now guess which auditors are most able to accommodate on cost – those that hire and retain competent professionals and diligently do their work or those that hire inexperienced and incompetent personnel to bury their head in the sand, omit procedures and ignore problems). Qualified and experienced professionals demand higher pay than their less qualified and experienced counterparts and, although you would expect efficiencies provided by competence and experience, those efficiencies are dwarfed by the efficiency of omitted procedures and fewer issues to deal with. Have less competent and experienced auditors ask fewer questions and do less corroboration and you find fewer or no problems. Auditors that have never heard of a TDR or risk-based capital or seen a loan file are not very likely to find problems in those areas.

Likewise, bankers that make sincere efforts to comply incur more costs than those that do not (both internally and from external sources) and practically are held to higher standards than those that do not. When a regulator enters an institution that is a mess, the magnitude of the problems subconsciously lower his or her expectations. When the situation is clean, then he/she has more time to dig-in.

No doubt some auditors rationalize that the limited liability provided by these engagement letter clauses actually do limit their risks and, therefore, do less work than is appropriate under GAAS. However, the actual legal protection afforded is questionable, especially since professionalism would preclude this approach because a professional auditor's assessment of these "business risks" should only expand the level of testing that is otherwise appropriate to the circumstances, it should never reduce the amount of work. The nature, timing and extent of audit procedures in a GAAS-compliant audit should be based on audit risks, not the auditor's business risks, and that is already part of GAAS. Anyone actually relying on these limited liability clauses to get out of professional performance has gained nothing but a false sense of security. However, due to lax enforcement, the real risk presented by any audit failure outside the public company arena is very small. I firmly believe the limited liability clauses are primarily reactive instead of proactive and the effect on auditor mindset is miniscule compared to the matters discussed above. Do you really believe bad, unprofessional auditors will suddenly rise to their professional responsibilities just because a few paragraphs are removed from engagement letters?

The FIL, under part *IV. Proposed Advisory*, subsection *Auditor Independence*, makes reference to SEC guidance in a December 13, 2004 FAQ which, in part, states "…seeks to provide the accountant immunity from liability for his or her own negligent acts, the accountant is not independent." Personally, I don't think any legal proceeding would be swayed to obviate an auditor's responsibility under GAAS by an engagement letter that included such language. Additionally, most of these "limited liability" clauses do not seek shelter from the auditor's own negligent acts (although some do), but rather from being held accountable for matters beyond the auditor's control and scope of the engagement. Surely the regulatory

agencies do not believe external auditors should be a second insurance fund that must step up and pay regardless of their responsibility? If that is the approach that develops, then the work done and fees charged will reflect that reality. That is also a very inefficient mechanism, because the big winners will be attorneys representing both sides and the results will be so far removed from the cause in terms of time that there will be no benefit in transforming mind sets.

Another problematic area is referenced in the FIL regarding management misrepresentations to auditors. Certainly auditor's should not accept management representations on their face, but any realistic expectations with a cost benefit consideration would realize that there is only so much an auditor can do and only so much that an auditor can find out about if management does not tell them. For example, how would an auditor find out about a contingent liability that is not recorded in the financial statements unless management conveys sufficient information for the auditor to recognize the issue?

In *Part IV. Proposed Advisory*, first paragraph in the *Auditor Independence* section, the FIL states "…the Agencies rules require only that an external auditor meet the AICPA independence standards…" Further, footnote 8 in the FIL states "AICPA Ethics ruling 94 (ET§191.188-189) currently concludes that indemnification for 'knowing misrepresentations by management' does not impair independence." Despite this clear guidance to the contrary, the FIL indicates that this type of clause impairs independence, objectivity and performance and also suggests that they may violate existing standards. Unfortunately, this is the type of contradictory guidance we have come to expect. It also exemplifies one reason for the diversity in practice and enforcement.

National efforts to make it illegal for management to lie to auditors failed, yet auditors are still expected to detect these lies – which by definition are fraud. Fraud, especially when perpetrated at the top by those with the ability to override controls and intimidate subordinates, is virtually impossible to detect unless someone talks. This is where the real problems lie anyway. Enron, WorldCom and hundreds of other "audit failures" evidenced by restatements weren't perpetrated by low level employees stealing pennies. They were perpetrated by senior management in intentional, concerted efforts to achieve their objectives. If you truly had independent auditors and AC's, I suggest that these "failures" would never have occurred, regardless of the state of internal controls. That is the real problem with this FIL, it addresses symptoms and not root causes.

So you have to decide, do you really want to fix the problem, or just keep pretending?

Another suggestion is to replace financial statement and internal control audits with call report audits. Regulators don't care about GAAP financial statements and footnotes. Do you even read them? I recently talked to a regulator that had done a review of a financial statement audit because we were proposing on the next audit. If the financial statements issued in the previous audit were any indication, these auditors had no clue. Among numerous errors and inconsistencies identified in a quick reading of the financial statements, I noticed there was no regulatory capital footnote and the financial statements presented two years, but several of the footnotes only had amounts for the prior year. This regulator had just completed a review and had found no problems with the audit.

Regulatory reporting (call reports) is required and designed for your purposes. An audit or *agreed-upon-procedures* on the call reports would raise the reliability of regulatory reporting. The FFIEC could specify the procedures to be performed, line-by-line as applicable to the various call report forms, and have external auditors perform those procedures. These procedures could also be scaled to CAMELS ratings. If a particular institution presents unusual risks, then appropriate procedures could be specified.

If you want cash, investments, loans, deposits and other borrowings confirmed with a third party, then specify confirmation of those line items. If you want loan review performed, then specify that procedure and the selection criteria. If you want risk-weightings audited, then specify that. If you want certain internal controls tested and evaluated, specify them. You simply list the procedures that are valuable to you and require them to be performed, on call report information. The extent of work performed would then increase and/or decrease in direct proportion to the complexity and size of the institution because of the additional regulatory reporting required based on those factors.

A GAAS audit has the auditor focused on a lot of issues and another set of financial statements and disclosures that YOU DO NOT CARE ABOUT – this means costs without benefits. You use the call reports, they are publicly available, generally contain more detail than audited financial statements and are generally available sooner than audited financial statements. Why waste time and money performing tasks and procedures no body cares about? This probably is not applicable to publicly-held holding companies, but would be just as relevant to the subsidiary institutions, especially since the external auditor could leverage these "agreed-upon-procedures" in their PCAOB audit of the holding company.

I must reemphasize my perspective that FIL 41-2005 is directed at a small symptom of the problem and not the cause. If you do not address the real issues, than all the band-aids in the world will not work (and this is barely a band-aid). Finally, please, please stop making chumps out of the people that strive to act professionally. Making more laws and new rules without enforcement is destined for the same result.

Sincerely,

Lam Vinson & Company, LLP

/s/ Russ Lam, CPA

Russ Lam, CPA